STATE of ARIZONA

Government Information Technology Agency	**Statewide STANDARD** P800-S890 Rev 1.0	**TITLE: Personnel Security** **Effective Date: April 5, 2004**

1. AUTHORITY

The Government Information Technology Agency (GITA) shall develop, implement and maintain a coordinated statewide plan for information technology (IT) (A.R.S. § 41-3504(A (1))) including the adoption of statewide technical, coordination, and security standards (A.R.S. § 41-3504(A (1(a)))).

2. PURPOSE

This standard defines requirements for protection of State IT assets from intentional misuse or destruction by State employees or contractors, who represent a potential source of unauthorized access and misuse of sensitive and confidential information.

3. SCOPE

This applies to all budget units. Budget unit is defined as a department, commission, board, institution or other agency of the state organization receiving, expending or disbursing state funds or incurring obligations of the state including the board of regents and the state board of directors for community colleges but excluding the universities under the jurisdiction of the board of regents and the community colleges under their respective jurisdictions and the legislative or judicial branches. A.R.S. § 41-3501(2).

The Budget Unit Chief Executive Officer (CEO), working in conjunction with the Budget Unit Chief Information Officer (CIO), shall be responsible for ensuring the effective implementation of Statewide Information Technology Policies, Standards, and Procedures (PSPs) within each budget unit.

4. STANDARD

The following standards provide requirements that protect information technology assets belonging to the State of Arizona from misuse or destruction by State employees and contractors.

4.1. WRITTEN POLICIES AND PROCEDURES: Budget units shall establish and document personnel security policies as well as related procedures that show clear accountability for security administration. Policies and procedures shall be applied to every existing State employee and contractor, as well as to new State employees and contractors, in order to prevent potential unauthorized access to and misuse of sensitive and confidential information. Policies and procedures shall be made available to all State employees and contractors and should be signed to indicate acceptance and understanding.

- The specific procedure which directs the steps and the timing required to grant or withdraw physical and system access privileges to State employees and contractors working for or on behalf of the budget unit shall be documented for the following events:

- New hire and/or new contractor staff/organization,
- Change of job duties within the agency,
- Transfer to another agency,
- Resignation,
- Termination, contract expiration, and
- Alleged inappropriate behavior (as defined by the budget unit).

4.2. DOCUMENTED ACCESS TO INFORMATION AND RESOURCES:

- System, application, and information access shall only be granted in accordance with a formal, written, and auditable procedure (including a formal, written request for access to specific systems or data). Granting of access should be accompanied by appropriate security training in accordance with *Statewide Standard P800-S895, Security Training and Awareness*.
- *Statewide Standard P800-S810, Account Management*, provides requirements for establishing and changing user accounts, classifications, and responsibilities.
- Users should be provided access to the minimum set of resources required for their role, to minimize the impact of any security violations and improve accountability. The principle of least privilege requires identifying what the user's job is, determining the minimum set of privileges required to perform that job, and restricting the user to those privileges and nothing more. Denying access to resources that are not necessary for the performance a user's duties prevents those denied privileges from being used to circumvent security policy and standards.
- Permissions, or rights, shall be granted in accordance with group or role membership(s) based on job functions and assignments.
- Access privileges shall be removed whenever an authorized user changes jobs or terminates employment.

4.2.1. Intellectual Property – access to intellectual property shall be granted only after fulfillment of requirements specified in *Statewide Policy P252, Intellectual Property and Fair Use*.

4.2.2. E-mail – e-mail access shall only be established in accordance with requirements provided in *Statewide Policy P401, E-Mail Use*.

4.2.3. Internet Access – Internet access shall only be established in accordance with requirements provided in *Statewide Policy P501, Internet Use.*

4.3. SEPARATION OF DUTIES: Where reasonably and economically feasible for a budget unit, the State employee or contractor in charge of security for a "like" group of IT devices or services should not be responsible for the security of other groups of IT devices or services. (For example, the individual establishing user accounts should not be the same individual that grants access to software applications and associated databases.)

4.4. EMPLOYMENT CONSIDERATIONS: Job-related requirements for potential IT personnel or contractors working in primary facilities housing critical

information systems or handling confidential information shall be a hiring consideration.

- Terms and conditions of employment and job descriptions should specify information security responsibilities.
- Budget units that perform fingerprint imaging shall adhere to current Arizona Department of Public Safety (DPS) standards for fingerprint imaging/identification.
- Non-Disclosure Agreements and applicable confidentiality and security agreements shall be signed by all State employees or contractors, who require access to confidential information, prior to their being granting access to that information.

5. DEFINITIONS AND ABBREVIATIONS

Refer to the PSP Glossary of Terms located on the GITA website at http://www.azgita.gov/policies_standards/ for definitions and abbreviations.

6. REFERENCES

6.1. A. R. S. § 41-621 et seq., "Purchase of Insurance; coverage; limitations, exclusions; definitions."
6.2. A. R. S. § 41-1335 ((A (6 & 7))),"State Agency Information."
6.3. A. R. S. § 41-1339 (A),"Depository of State Archives."
6.4. A. R. S. § 41-1461, "Definitions."
6.5. A. R. S. § 41-1463, "Discrimination; unlawful practices; definition."
6.6. A. R. S. § 41-1492 et seq., "Prohibition of Discrimination by Public Entities."
6.7. A. R. S. § 41-2501 et seq., "Arizona Procurement Codes, Applicability."
6.8. A. R. S. § 41-3501, "Definitions."
6.9. A. R. S. § 41-3504, "Powers and Duties of the Agency."
6.10. A. R. S. § 41-3521, "Information Technology Authorization Committee; members; terms; duties; compensation; definition."
6.11. A. R. S. § 44-7041, "Governmental Electronic Records."
6.12. Arizona Administrative Code, Title 2, Chapter 7, "Department of Administration Finance Division, Purchasing Office."
6.13. Arizona Administrative Code, Title 2, Chapter 10, "Department of Administration Risk Management Section."
6.14. Arizona Administrative Code, Title 2, Chapter 18, "Government Information Technology Agency."
6.15. Statewide Policy P100, Information Technology.
6.16. Statewide Policy P252, Intellectual Property and Fair Use.
6.17. Statewide Policy P401, E-Mail Use.
6.18. Statewide Policy P501, Internet Use.
6.19. Statewide Policy P800, IT Security.
  6.19.1. Statewide Standard P800-S810, Account Management.
  6.19.2. Statewide Standard P800-S895, Security Training and Awareness.
6.20. State of Arizona Target Security Architecture, http://www.azgita.gov/enterprise_architecture.

7. ATTACHMENTS

None.